Journal of Number Theory 129 (2009) 1443–1455

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the power-free values of polynomials in two variables: II

C. Hooley

Cardiff School of Mathematics, Cardiff University, Senghennydd Road, Cardiff, CF24 4AG, United Kingdom

ARTICLE INFO

Article history:
Received 21 May 2008
Available online 26 March 2009
Communicated by Gebhard Böckle

Dr. Greaves in memoriam

ABSTRACT

The following theorem is proved. Suppose that for integers $r, s \geqslant 2$, $f(x, y)$ is an inhomogeneous polynomial of degree r with rational integral coefficients that is irreducible over the rationals, that is not a polynomial in a linear combination of x and y, that has no fixed sth power divisors other than 1, and that is a product of linear factors over some extension field of the rationals. Then, if $N(X)$ denote the number of integers m, n of magnitude not exceeding X for which $f(m, n)$ is sth power-free, the asymptotic formula

$$N(X) \sim 4X^2 \prod_p \left(1 - \frac{\rho(p^s)}{p^{2s}}\right)$$

is valid for $s \geqslant \frac{1}{2}r - 1$, where $\rho(l)$ is the number of incongruent zeros, mod l, of $f(x, y)$. In these circumstances $f(m, n)$ is infinitely often sth power-free.

This result improves upon a lower bound found for $N(X)$ in a previous paper [C. Hooley, On the power-free values of polynomials in two variables, Roth 80th birthday volume, in press].

1. Introduction

In the first paper with the above title [2], to which we shall refer as I and to which we direct the reader for background information on the topic, we responded to a query from Dr. Greaves by proving the truth of the following

Statement. *Suppose that for integers $r, s \geqslant 2$, $f(x, y)$ is an inhomogeneous polynomial of degree r with rational integral coefficients that is irreducible over the rationals, that is not a polynomial in a linear combination*

E-mail address: millsme@cardiff.ac.uk.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.12.006

of x and y, and that has no fixed sth power divisors other than 1, *there being two possible cases* (A) *or* (B) *according as $f(x, y)$ is not or is a product of linear factors over some extension field of the rationals. Then, if $N(X)$ denote the number of integers m, n of magnitude not exceeding X for which $f(m, n)$ is sth power-free, the inequality*

$$N(X) > 4cX^2 \prod_p \left(1 - \frac{\rho(p^s)}{p^{2s}}\right) \quad (X > X_0)$$

is valid for $s \geqslant \frac{3}{4}r - 1$ in case (A) *and for $s \geqslant \frac{1}{2}r - 1$ in case* (B), *where $\rho(l)$ is the number of incongruent zeros,* mod l, *of $f(x, y)$ and c is a positive constant less than* 1 *that depends only on the case* (A) *or* (B) *in question.*

In these circumstances $f(m, n)$ is infinitely often sth power-free.

Thus, with an improved range of s for each degree r, we extended to inhomogeneous polynomials in two variables the results for those in one variable that have been the subject of interest and attention over many years, although the asymptotic formulae usual in the latter situation were replaced by lower bounds for $N(X)$ of the expected order of magnitude. But in the third footnote in I we stated that it was conceivable that even an asymptotic formula for $N(X)$ could be substantiated in case (B). This belief we have now vindicated and we therefore now intend to prove a formula of the type

$$N(X) \sim A(f)X^2 \quad \big(A(f) > 0\big)$$

as $X \to \infty$ when $f(x, y)$ conforms to case (B) in the circumstances delineated in the statement above and, in particular, to the condition $s \geqslant \frac{1}{2}r - 1$.

Though a new idea is needed to implement the improvement, much of the treatment depends on explanations and estimations from the former paper. To avoid undue repetition of what went before we therefore refer frequently to I, while dilating sufficiently on some points in the previous exposition to enable the reader to pick up the present narrative without undue trouble. As we shall see the main departure from I is in the replacement of the sum $N^{(4)}(x)$ there by a new sum $\mathcal{N}^{(4)}(x)$ that is connected with the divisibility of $f(m, n)$ by the squares of primes. Indeed, it is in the treatment of the consequential congruences, mod p^2, and the concomitant exponential sums that the principal task of the exposition lies.

Actually, it is not difficult to replace the asymptotic formula by an equality for $N(X)$ containing a remainder term. But this would involve a substantial remodelling of the analysis that we would be loath to undertake because of the slightness of the improvement.

We end by stating without proof an asymptotic formula for the cardinalities of cube-free values of binary octic forms, thus dealing as explained in I with a situation left untouched by Greaves and Filaseta.

2. Notation

The letters a, b (with or without additional adornments such as subscripts), m, n, μ, ν usually denote integers; d, h, l are positive integers; p is a (positive) prime number.

The letters $A, A_1, A_2, \ldots$ are positive constants depending at most on the given polynomial; C is an arbitrarily large constant; X is a variable to be regarded as tending to infinity, all relations stated being valid when it is large enough; the constants implied by the O-notation depend at most on C and the given polynomial.

3. Initial comments and decomposition of sum

It will be assumed until the very end of the paper that $f(x, y)$ satisfies the condition specified in the Statement of Section 1 for case (B) so that $f(x, y)$ is an irreducible polynomial that is a rational multiple of a product of (distinct) linear factors over some extension field of the rationals. Also, not only shall we assume that

$$s \geqslant \frac{1}{2}r - 1 \tag{1}$$

but that also, if necessary, $s < r - 1$ because traditional methods will treat the complementary case $s \geqslant r - 1$. Thus attention is restricted to polynomials of degree $r \geqslant 4$; also, in line with comments in I, Section 3, the full power of the method is only needed for the smallest value of s in (1).

Of the two parameters ξ_1, ξ_2 defined in I (7), we shall only need the latter, which as before is given by

$$\xi_2 = X^2 \log^{\frac{9}{10}} X. \tag{2}$$

To this we again adjoin a large positive constant C, on which the constants implied by the O-notation may depend and which now will ultimately be allowed to tend to infinity. Then, the sum $N(X)$ being the number of pairs of integers m, n of magnitude not more that X for which $f(m, n)$ is sth power-free, we analyze it in terms of other sums that also count pairs m, n of like size for which $f(m, n)$ and m, n have certain stated attributes. But to achieve this we must anticipate later developments by affirming that, for each suitable prime p, special rôles will be played by pairs (m, n) that belong to certain systems $\mathcal{S}_p$, $\mathcal{S}_p^{(1)}$ of not more than $R = R(r)$, $R_1 = R_1(r)$ respective residue classes, mod p, where

$$\mathcal{S}_p \subset \mathcal{S}_p^{(1)}; \tag{3}$$

here $\mathcal{S}_p$ is the same as in I except that it is used over a longer range of p, while the meaning of $\mathcal{S}_p^{(1)}$ will emerge in Section 5. The designations and defining features of the sums we introduce are then as follows:

(i) $N_l(X)$ – $f(m, n)$ is divisible by the positive integer l;
(ii) $N^{(1)}(X)$ – $f(m, n)$ is indivisible by the sth power of any prime not exceeding C;
(iii) $\mathcal{N}^{(3)}(X)$ – the pair (m, n) belongs to $\mathcal{S}_p^{(1)}$ for some p in the range $C < p \leqslant \xi_2$;
(iv) $\mathcal{N}_{p^2,p}(X)$ – $f(m, n)$ is divisible by p^2 but (m, n) does not belong to $\mathcal{S}_p^{(1)}$;
(v) $\mathcal{N}^{(4)}(X)$ – $f(m, n)$ is divisible by the square of some prime p in the range $C < p \leqslant \xi_2$ but (m, n) does not belong to any $\mathcal{S}_p^{(1)}$ for any p in this range;
(vi) $\mathcal{N}^{(5)}(X)$ – $f(m, n)$ is divisible by the sth power of some prime p exceeding ξ_2 but is indivisible by p^s for $p \leqslant C$ and by p^2 for $C < p \leqslant \xi_2$; also (m, n) does not belong to $\mathcal{S}_p$ for $C < p \leqslant \xi_2$.

Then, in the spirit of the *simple asymptotic sieve* as described in Chapter 1 of our tract [1], the two inequalities

$$N(X) \leqslant N^{(1)}(X)$$

and

$$N(X) \geqslant N^{(1)}(X) - \mathcal{N}^{(3)}(X) - \mathcal{N}^{(4)}(X) - \mathcal{N}^{(5)}(X)$$

imply the inequality

$$\left|N(X) - N^{(1)}(X)\right| \leqslant \mathcal{N}^{(3)}(X) + \mathcal{N}^{(4)}(X) + \mathcal{N}^{(5)}(X), \tag{4}$$

on which some initial comment should be made before its constituents are estimated.

Of the sums appearing in (4), the only one apart from $N(x)$ that is the same as one in the counterpart equation (8) in I is $N^{(1)}(X)$; the others are merely analogues of the previous sums $N^{(3)}(X)$, $N^{(4)}(X)$, and $N^{(5)}(X)$ and are therefore distinguished from them by a change in the font of the initial

notational symbol. Here $\mathcal{N}^{(3)}(X)$ is similar to $N^{(3)}(X)$ save that the wider set $\mathcal{S}_p^{(1)}$ replaces $\mathcal{S}_p$ and the range of p is extended. Also part of $\mathcal{N}^{(4)}(X)$ subsumes the previous function of $N^{(2)}(X)$, while the complementary portion is essentially smaller and harder to estimate than $N^{(4)}(X)$ because the divisibility of $f(m,n)$ by p^2 is now in question; in fact, as already intimated, it is in this sum that the principal difficulty lies. Finally, there is only a slight departure of $\mathcal{N}^{(5)}(X)$ from $N^{(5)}(X)$ in both definition and treatment.

In dealing with $\mathcal{N}^{(4)}(X)$ (and implicitly $\mathcal{N}^{(5)}(X)$ through the method of I to be quoted) we continue the practice of introducing sums affected by functions $\gamma(u) = g_{c_1}(C_1 u/X)$ defined in I, Section 5, to which the reader is referred for details regarding their place in the method. But now the demand placed on them is rather less than before because the small bound found for $\mathcal{N}^{(4)}(X)$ can be changed to within a bounded multiple without detriment, whereas that found before for $N^{(4)}(X)$ had to be as small as possible in order not to vitiate the effect of $N^{(1)}(X)$ on the size of $N(X)$. Thus, instead of being large and ultimately tending to infinity, the constant C_1 may be defined by

$$C_1 = 1 \tag{5}$$

throughout the analysis of $\mathcal{N}^{(4)}(X)$, the caution that the O-constants might depend on it being now superfluous. Also involved in the estimation of $\mathcal{N}^{(4)}(X)$ (and implicitly of $\mathcal{N}^{(5)}(X)$) are the sums of the type $M_l^*(X)$ whose description and treatment are again to be found in I, Section 5. These are partial surrogates for the sums $N_l(X)$ and $\mathcal{N}_{p^2,p}(X)$ that are taken over families of solutions of congruences $f(m,n) \equiv 0$, modulis l and p^2. Accordingly we first dispose of the easier sums $N^{(1)}(X)$, $\mathcal{N}^{(3)}(X)$, and $\mathcal{N}^{(5)}(X)$ with the aid of I before going onto $\mathcal{N}^{(4)}(X)$.

4. The sums $N^{(1)}(X)$, $\mathcal{N}^{(3)}(X)$, and $\mathcal{N}^{(5)}(X)$

First, on returning to $N^{(1)}(X)$ we should be reminded that $\rho(l)$ in I denoted the number of incongruent zeros of $f(x,y)$, mod l, where according to Lemma 1 in I

$$\rho(\rho^j) = O\big(p^{2j-2}\big) \tag{6}$$

for $j \geqslant 2$ and where $\rho(\rho^s) < p^{2s}$ by our assumptions on $f(x,y)$. Then from the equation

$$N^{(1)}(X) = 4X^2 \prod_{p \leqslant C} \left(1 - \frac{\rho(p^s)}{p^{2s}}\right) + O(X)$$

in I(12), we deduce the required inequality

$$\left| N^{(1)}(X) - 4X^2 \prod_{p} \left(1 - \frac{\rho(p^s)}{p^{2s}}\right) \right| < \frac{AX^2}{C} \quad \big(X > X_0(C)\big) \tag{7}$$

concerning $N^{(1)}(X)$ because

$$1 > \prod_{p>C} \left(1 - \frac{\rho(p^s)}{p^{2s}}\right) > \prod_{p>C} \left(1 - \frac{A_1}{p^2}\right) > 1 - \frac{A_2}{C}$$

by (6).

Secondly, by the definition of $\mathcal{N}^{(3)}(X)$ in (iii), Section 3 and then by (2),

$$\begin{aligned}
\mathcal{N}^{(3)}(X) &\leqslant \sum_{C<p\leqslant\xi_2} \sum_{\substack{|m|,|n|\leqslant X\\ (m,n)\in\mathcal{S}_p^{(1)}}} 1 = \sum_{C<p\leqslant\xi_2} \sum_{\substack{0<\mu,\nu\leqslant p\\ (\mu,\nu)\in\mathcal{S}_p^{(1)}}} \sum_{\substack{|m|,|n|\leqslant X\\ m-\mu\equiv n-\nu\equiv 0,\bmod p}} 1\\
&\leqslant \sum_{C<p\leqslant\xi_2} \sum_{\substack{0<\mu,\nu\leqslant p\\ (\mu,\nu)\in\mathcal{S}_p^{(1)}}} \left(\frac{2X+1}{p}+O(1)\right)^2\\
&\leqslant A_3 \sum_{C<p\leqslant\xi_2} R_1(r)\left(\frac{X^2}{p^2}+1\right)\\
&< A_4X^2\sum_{p>C}\frac{1}{p^2}+A_4\sum_{p\leqslant\xi_2}1\\
&< \frac{A_5X^2}{C}+\frac{A_5X^2}{\log^{\frac{1}{10}}X} < \frac{AX^2}{C}. \qquad (8)
\end{aligned}$$

The assessment of $\mathcal{N}^{(5)}(X)$ only differs from that of $N^{(5)}(X)$ in case (B) in the early part of the treatment; here, as in I, the value of the constant C_1 is static and could indeed be taken to be 1 as in (5). By analogy with I (64), $\mathcal{N}^{(5)}(X)$ does not exceed the number of solutions in integers m, n, Q and positive primes q of both the primary conditions

$$f(m,n) = Qq^s; \qquad q>\xi_2; \quad |m|,|n|\leqslant X$$

and the secondary conditions

(a) Q is indivisible by the sth powers of primes not exceeding C and by the squares of primes between C (exclusive) and ξ_2 (inclusive),
(b) (m,n) does not belong to $\mathcal{S}_p$ for $C<p\leqslant\xi_2$, where $\mathcal{S}_p$ is exactly the same as in I.

Once again, with

$$\xi_3 = A_6X^2\log^{-\frac{9}{5}}X,$$

we have by (2) that

$$0<|Q|\leqslant\xi_3, \qquad Q=\pm l_1l_2, \quad (l_1,l_2)=1,$$

where $\pm l_1$ has prime divisors not exceeding C. Also, since $\xi_3<\xi_2$ by (2), the number l_2 is square-free in virtue of the secondary condition (a) and has prime factors p for each of which (m,n) does not pertain to $\mathcal{S}_p$. We thus, by slightly different reasoning, recoup exactly the same conclusion about l_2 as we did in I when stating equation (66) therein.

From this point on the handling of $N^{(5)}(X)$ in case (B) is applicable to $\mathcal{N}^{(5)}(X)$ and we therefore conclude as in I, Section 11 that

$$\mathcal{N}^{(5)}(X) = o\big(X^2\big) < \frac{AX^2}{C}. \qquad (9)$$

In particular, we should note that the family $\mathcal{S}_p$ used in the reasoning is the same as the one in I.

5. Preparations for the estimation of $\mathcal{N}^{(4)}(X)$

Whereas the treatment of $N^{(4)}(X)$ in I depended mainly on the properties of the congruence $f(x, y) \equiv 0$, mod p, that of $\mathcal{N}^{(4)}(X)$ relates to the harder congruence

$$f(x, y) \equiv 0, \text{ mod } p^2. \tag{10}$$

Not only do we now have to consider the reduction of $f(x, y)$, mod p, but also the properties of $f(x, y)$ when regarded as a polynomial over the p-adic field $\mathbb{Q}_p$, in which guise we find it convenient to term it the *p-adic reduction* of $f(x, y)$. Consequently, we extend the initial convention in I, Section 6 by occasionally following the practice of using the same symbol for a rational integer, the element in the finite field $\mathbb{F}_p$ to which it gives rise through the residue class, mod p, containing it, and the corresponding element in $\mathbb{Z}_p$.

First we know from I, Section 6 that, with suitable non-zero integers B, B_1 (whose prime divisors are less than C), we may write

$$B_1 f(x, y) = \prod_{1 \leqslant i \leqslant r} \left(Bx + \theta_i y + \theta_i'\right),$$

in which the pairs θ_i, θ_i' are simultaneous conjugates of algebraic integers θ, θ' with respect to a super-field $\mathbb{Q}(\theta, \theta') = \mathbb{Q}(\phi)$ defined by an algebraic integer ϕ of degree r over $\mathbb{Q}$. In fact, by a minor adjustment to B and B_1 if necessary,

$$B_1 f(x, y) = \prod_{1 \leqslant i \leqslant r} \left(Bx + u(\phi_i) y + v(\phi_i)\right), \tag{11}$$

where $u(\phi)$ and $v(\phi)$ are polynomials in ϕ with rational *integral* coefficients. Also the homogeneous portion of $Bf(x, y)$ of degree r is B_1 an (r/w)th power of an irreducible binary form $F(x, y)$ of degree $w > 1$.

Next we examine the factorizations of the two reductions of $f(x, y)$ over the algebraic closures of $\mathbb{F}_p$ and $\mathbb{Q}_p$. To this end let the monic minimum polynomial of ϕ (with integral coefficients) be $\psi(t)$ and, regarding its respective reductions, mod p, and p-adically, let its zeros in $\bar{\mathbb{F}}_p$ and $\bar{\mathbb{Q}}_p$ be $\upsilon_1, \ldots, \upsilon_r$ and $\Upsilon_1, \ldots, \Upsilon_r$. Then, since any elementary symmetric function in $\upsilon_1, \ldots, \upsilon_r$ is the element in $\mathbb{F}_p$ defined by the integer that is the corresponding symmetric function in $\phi_1, \ldots, \phi_r$, we have by comparison with (11) that

$$B_1 f(x, y) = \prod_{1 \leqslant i \leqslant r} \left(Bx + u(\upsilon_i) y + v(\upsilon_i)\right) = \prod_{1 \leqslant i \leqslant r} (Bx + u_i y + v_i), \quad \text{say}, \tag{12}$$

in $\bar{\mathbb{F}}_p$, while similarly but more obviously

$$B_1 f(x, y) = \prod_{1 \leqslant i \leqslant r} \left(Bx + u(\Upsilon_i) y + v(\Upsilon_i)\right) = \prod_{1 \leqslant i \leqslant r} (Bx + U_i y + V_i), \quad \text{say}, \tag{13}$$

in $\bar{\mathbb{Q}}_p$. Moreover, the factors in (12) are distinct by the comments in I, Section 6, as are those in (13) because the characteristic of $\mathbb{Q}_p$ is zero. It then follows as in I that the pairs (u_i, v_i) appertain to $\mathbb{F}_p$ if and only if $\upsilon_i \in \mathbb{F}_p$, the same reasoning shewing that the pairs (U_i, V_i) relate to $\mathbb{Q}_p$ if and only if $\Upsilon_i \in \mathbb{Q}_p$, in which event U_i, V_i belong to $\mathbb{Z}_p$ because $\psi(t)$ is monic.

In the notation of I let $\tau(p)$ still denote the number of incongruent roots, mod p, of

$$\psi(t) \equiv 0, \text{ mod } p,$$

and let us order the zeros of $\psi(t)$ in $\bar{\mathbb{F}}_p$ so that the first $\tau(p)$ subscripts i indicate the υ_i that belong to $\mathbb{F}_p$ Then, for $p > C$ so that p does not divide the discriminant of $\psi(t)$, take a residue t_i, mod p, within an υ_i for $i \leqslant \tau(p)$ and, in the spirit of the ideas behind Hensel's Lemma, construct in succession solutions $t_{i,\alpha}$ of

$$\psi(t) \equiv 0, \text{ mod } p^{\alpha},$$

for which $t_{i,1} = t_i$, $t_{i,\alpha+1} \equiv t_{i,\alpha}$, mod p^{α}, with the outcome that we find a zero in $\mathbb{Z}_p$ of $\psi(t)$ that can be denoted by Υ_i With this construction the first $\tau(p)$ indices i give values of U_i and V_i in (13) that belong to $\mathbb{Z}_p$; no other pair U_i, V_i in (13) can belong to $\mathbb{Z}_p$, since otherwise Υ_i would also belong to $\mathbb{Z}_p$ and this would give rise to an υ_i in $\mathbb{F}_p$ that would differ from $\upsilon_1, \ldots, \upsilon_{\tau(p)}$ by principles related to Hensel's Lemma. Thus (12) and (13) can be expressed as

$$\begin{aligned} B_1 f(x, y) &= \prod_{1 \leqslant i \leqslant \tau(p)} (Bx + u_i y + v_i) \prod_{\tau(p) < i \leqslant r} (Bx + u_i y + v_i) \\ &= f_1(x, y) f_2(x, y), \text{ say,} \end{aligned} \tag{14}$$

in $\overline{\mathbb{F}_p}$ and

$$\begin{aligned} B_1 f(x, y) &= \prod_{1 \leqslant i \leqslant \tau(p)} (Bx + U_i y + V_i) \prod_{\tau(p) < i \leqslant r} (Bx + U_i y + V_i) \\ &= f_1^*(x, y) f_2^*(x, y), \quad \text{say,} \end{aligned} \tag{15}$$

in $\overline{\mathbb{Q}_p}$; here $f_1(x, y) \in \mathbb{F}_p[x, y]$, $f_1^*(x, y) \in \mathbb{Z}_p[x, y]$ and therefore $f_2(x, y) \in \mathbb{F}_p[x, y]$, $f_2^*(x, y) \in \mathbb{Q}_p[x, y]$, whence actually $f_2^*(x, y) \in \mathbb{Z}_p[x, y]$ as $\psi(t)$ is monic.

Let us examine the implications of the p-adic equation (15) when we take the congruences, mod p^2, that lie within it. We get

$$B_1 f(x, y) \equiv \prod_{1 \leqslant i \leqslant \tau(p)} (Bx + U_i y + V_i) f_2^*(x, y), \text{ mod } p^2, \tag{16}$$

on transferring the polynomial coefficients implied by the notation from p-adic numbers to integers congruent to them, mod p^2. Also, now interpreting $f_1(x, y)$, $f_2(x, y)$ in $\mathbb{F}_p[x, y]$ as polynomials, mod p, we have [1]

$$f_2(x, y) \equiv f_2^*(x, y), \text{ mod } p, \tag{17}$$

because $f_1(x, y) \equiv f_1^*(x, y)$, mod p, by the connections between υ_i and Υ_i for $i \leqslant \tau(p)$.

In managing the congruence (16) for the assessment of $\mathcal{N}^{(4)}(X)$ we deliberately strike out a certain class of its solutions, although later it will be appropriate to restore some of these to the extent that they may even appear with a multiplicity greater than 1. We shall in fact initially agree not to count those that are either

(i) zeros of $f_2^*(x, y)$, mod p, or
(ii) simultaneous zeros, mod p, of two factors $Bx + U_i y + V_i$ for which $i \leqslant \tau(p)$ (or equally well, of two factors $Bx + u_i y + v_i$.)

[1] To obtain this congruence we have deliberately adopted a procedure that avoids substantial use of what Nineteenth Century writers would have termed the *imaginary* roots of $\psi(t) \equiv 0$, mod p.

In case (i), by (17), the zeros omitted correspond to the solutions in $\mathbb{F}_p$ of $f_2(x, y) = 0$. Since in each factor of $f_2(x, y)$ as exhibited in (14) not both u_i and v_i belong to $\mathbb{F}_p$, the number of these zeros does not exceed 1 and therefore the number of incongruent elements, mod p, in category (i) does not exceed $R_1^{(1)}(r)$. Similarly, by considering simultaneous equations, the number of elements, mod p, in category (ii) does not exceed $R_2^{(1)}(r)$, where we then set $R^{(1)}(r) = R_1^{(1)}(r) + R_2^{(1)}(r)$.

The constituents thus excluded are to form the set $\mathcal{S}_p^{(1)}$ of residue classes that was introduced in the preamble to Section 3, it being confirmed that (3) holds because in I, Section 6 the set $\mathcal{S}_p$ was contained in the set of residue classes, mod p, defined by (i).

From (16) it is then evident that the solutions of (10) that do not conform to $\mathcal{S}_p^{(1)}$ answer to a set $\mathcal{J}_{p^2}$ of residue class pairs that correspond to the zeros, mod p^2, of one, and only one, of the linear congruences

$$Bx + U_i y + V_i \equiv 0, \mod p^2. \tag{18i}$$

Also important in what follows is the p-adic equation

$$\big\{F(x, y)\big\}^{r/w} = \prod_{1 \leqslant i \leqslant r} (Bx + U_i y)$$

that stems from (13) and the definition of $F(x, y)$. Hence, for $i \leqslant \tau(p)$, $Bx + U_i y$ is a divisor of $F(x, y)$, from which fact it follows (most easily by long division) that

$$B_2 F(x, y) = (Bx + U_i y)\Psi_i(x, y)$$

with $p \nmid B_2$ and $\Psi_i(x, y) \in \mathbb{Z}_p[x, y]$. Therefore, with the notational convention previously used in (16),

$$B_2 F(x, y) \equiv (Bx + U_i y)\Psi_i(x, y), \mod p^2 \quad (p \nmid B_2). \tag{19}$$

With the attitude of the third paragraph of Section 5 in I, let us introduce the concept of a family $\mathcal{R}_{p^2}^{(1)}$ of residue pairs μ, ν with $0 < \mu, \nu \leqslant p^2$ and cardinality $\kappa^*(p^2)$ that are not necessarily distinct, or more precisely, of residue pairs μ_i, ν_i with $0 < \mu_i, \nu_i \leqslant p^2$ that are indexed by a subscript i running from 1 to $\kappa^*(p^2)$. Then in the present instance the family $\mathcal{R}_{p^2}^{(1)}$ we use is to be the aggregate of all solutions μ_i, ν_i of (18i) for $i \leqslant \tau(p)$ and for which $0 < \mu_i, \nu_i \leqslant p^2$, it then being evident that $\mathcal{R}_{p^2}^{(1)}$ covers the set $\mathcal{J}_{p^2}$. Moreover, by I(21), the apposite sum of type $M_l^*(X)$ we shall need in the estimation of $\mathcal{N}^{(4)}(X)$ will be

$$\mathcal{M}_{p^2}^*(X) = \sideset{}{^*}\sum_{(\mu,\nu)\in\mathcal{R}_{p^2}^{(1)}} \sum_{\substack{m\equiv\mu, \bmod p^2\\ n\equiv\nu, \bmod p^2}} \gamma(m)\gamma(n),$$

which has the valuable property that

$$\mathcal{N}_{p^2,p}(X) \leqslant \mathcal{M}_{p^2}^*(X) \tag{20}$$

by the definition of $\mathcal{N}_{p^2,p}(X)$ in (iii), Section 3 and the fact that $\gamma(t)$ bounds the characteristic function of the interval $|t| \leqslant X$. Next, to use $\mathcal{M}_{p^2}^*(X)$ we need its development

$$\frac{9X^2\kappa^*(p^2)}{p^4} + O\bigg(\frac{X^2}{p^4} \sideset{}{'}\sum_{|a|,|b|\leqslant p^2/X} \big|E^*\big(a, b; p^2\big)\big|\bigg) \tag{21}$$

given by I(24) with $C_1 = 1$, where $E^*(a, b; p^2)$ is the exponential sum

$$\sum_{\mu,\nu\in\mathcal{R}^{(1)}_{p^2}} e^{2\pi i(a\mu+b\nu)/p^2}$$

and the prime symbol over the summation symbol indicates that the pair $(0, 0)$ is omitted.

The first part of our preparations for the estimation of $\mathcal{N}^{(4)}(X)$ lies in the treatment of $E^*(a, b; p^2)$ and $\kappa^*(p^2)$. By the definition of $\mathcal{R}^{(1)}_{p^2}$

$$\begin{aligned} E^*\big(a, b; p^2\big) &= \sum_{1\leqslant i\leqslant\tau(p)} \sum_{\substack{B\mu+U_i\nu+V_i\equiv 0,\ \mathrm{mod}\ p^2\\ 0<\mu,\nu\leqslant p^2}} e^{2\pi i(a\mu+b\nu)/p^2} \\ &= \sum_{1\leqslant i\leqslant\tau(p)} E_i^*\big(a, b; p^2\big), \quad \text{say.} \end{aligned} \tag{22}$$

Next let $\bar{B}$ be any number with the property that $B\bar{B}\equiv 1,\ \mathrm{mod}\ p^2\ (p > C)$. Then the main condition of summation in $E_i^*(a, b; p^2)$ is tantamount to

$$\mu \equiv -\bar{B}U_i\nu - \bar{B}V_i,\ \mathrm{mod}\ p^2,$$

with the inference that

$$E_i^*\big(a, b; p^2\big) = e^{-2\pi i a\bar{B}V_i/p^2} \sum_{0<\nu\leqslant p^2} e^{2\pi i(b-a\bar{B}U_i)\nu/p^2},$$

the right-side of which equation has magnitude 0 or p^2 according as $bB - aU_i \not\equiv 0,\ \mathrm{mod}\ p^2$, or $bB - aU_i \equiv 0,\ \mathrm{mod}\ p^2$. Since the latter condition implies that $F(b, -a)\equiv 0,\ \mathrm{mod}\ p^2$, by (19), we see that $E_i^*(a, b; p^2) = 0$ unless $F(b, -a)\equiv 0,\ \mathrm{mod}\ p^2$, in which case its magnitude does not exceed p^2. Hence

$$\big|E^*\big(a, b; p^2\big)\big| \begin{cases} \leqslant rp^2, & \text{if } p^2 \mid F(b, -a), \\ = 0, & \text{if } p^2 \nmid F(b, -a), \end{cases} \tag{23}$$

with the special implication that

$$\kappa^*\big(p^2\big) \leqslant rp^2. \tag{24}$$

6. Estimation of $\mathcal{N}^{(4)}(X)$

By definitions (iv) and (v) in Section 3 and then by (20), we have

$$\mathcal{N}^{(4)}(X) \leqslant \sum_{C<p\leqslant\xi_2} \mathcal{N}_{p^2,p}(X) \leqslant \sum_{C<p\leqslant\xi_2} \mathcal{M}^*_{p^2}(X)$$

and therefore

$$\mathcal{N}^{(4)}(X) \leqslant 9X^2 \sum_{C<p\leqslant\xi_2} \frac{\kappa^*(p^2)}{p^4} + O\left(X^2 \sum_{C<p\leqslant\xi_2} \frac{1}{p^4} \sum_{0\leqslant|a|,|b|\leqslant p^2/X}{}' \left|E^*(a,b;p^2)\right|\right)$$
$$= 9X^2 P_1(X) + O\left(X^2 P_2(X)\right), \text{ say,} \tag{25}$$

after using (21). In this at once

$$P_1(X) \leqslant r \sum_{p>C} \frac{1}{p^2} < \frac{A}{C} \tag{26}$$

by (24). Next let us examine the contribution to $P_2(X)$ due to those values of p, a, b for which $p \mid a$, $p \mid b$ and for which therefore $a = pa_1$, $b = pb_1$, and $|a_1|, |b_1| \leqslant p/X$. This, by (23), is

$$O\left(\sum_{X\leqslant p\leqslant\xi_2} \frac{1}{p^2} \sum_{0\leqslant|a_1|,|b_1|\leqslant p/X}{}' 1\right) = O\left(\frac{1}{X^2}\sum_{p\leqslant\xi_2} 1\right) = O\left(\frac{\xi_2}{X^2\log\xi_2}\right) = O\left(\frac{1}{\log^{\frac{1}{10}} X}\right) \tag{27}$$

because of (2).

For the remaining portion $P_2'(X)$ of $P_2(X)$ we shall need Lemma 5 of I, which for convenience we repeat as the

Lemma. *The number of primitive solutions of the congruence*

$$du \equiv v, \bmod q \quad (d \neq 0),$$

for which $|u|, |v| \leqslant U$ *is*

$$O\left(\frac{U^2}{q}\right) + O(1).$$

There being no contribution to $P_2'(X)$ from values of p less than $\sqrt{X}$, the effect on it of primes p within the summation for which $u < p \leqslant 2u$ $(\frac{1}{2}\sqrt{X} < u < \xi_2)$ is

$$O\left(\frac{1}{u^2}\sum_{u<p\leqslant 2u} \sum_{\substack{|a|,|b|\leqslant 4u^2/X \\ F(b,-a)\equiv 0, \bmod p^2 \\ (a,b,p)=1}}{}' 1\right) = O\left(\frac{1}{u^2}\sum\nolimits_u\right), \quad \text{say,} \tag{28}$$

by the estimate (23). Next, if we set $d = (a, b)$ in the inner sum within $\sum_u$ so that $a = da'$, $b = db'$, $(a', b') = 1$, and $p \nmid d$, it follows that

$$\sum\nolimits_u \leqslant \sum_{u<p\leqslant 2u} \sum_{d\leqslant 4u^2/X} \sum_{\substack{|a'|,|b'|\leqslant 4u^2/Xd \\ F(b',-a')\equiv 0, \bmod p^2 \\ (a',b')=1}} 1$$
$$= \sum_{d\leqslant 4u^2/X} \sum_{u<p\leqslant 2u} \sum_{\substack{|a'|,|b'|\leqslant 4u^2/Xd \\ F(b',-a')\equiv 0, \bmod p^2 \\ (a',b')=1}} 1$$
$$= \sum_{d\leqslant 4u^2/X} \sum\nolimits_{u,d}', \quad \text{say,} \tag{29}$$

which inequality we exploit by considering separately the two cases

$$\eta < d \leqslant 4u^2/X, \quad d \leqslant \eta$$

for a suitable choice of $\eta = \eta(X, u)$.

In the first case, the form $F(x, y)$ being irreducible and of degree exceeding 1, we have

$$\sum\nolimits_{u,d} \leqslant \sum_{|a'|,|b'| \leqslant 4u^2/Xd}{}' \sum_{\substack{p^2 | F(b', -a') \\ p > u}} 1 = O\left(u^4/X^2d^2\right) \tag{30}$$

because the non-zero value of $F(b', -a')$ can only have a bounded number of prime factors exceeding $u > \frac{1}{2}\sqrt{X}$. But in the second case we look at the congruence in the definition of $\sum_{u,d}$ by (29) and note that, p being large, its coprime solutions obey a relation

$$a'\omega \equiv -b', \mod p^2,$$

where $\omega \neq 0$ is one of the bounded number of incongruent solutions of $F(\omega, 1) \equiv 0$, mod p^2. Therefore by the lemma we obtain the alternative estimate

$$\begin{aligned} \sum\nolimits_{u,d} &= O\left\{ \sum_{u < p \leqslant 2u} \left(\frac{u^4}{X^2d^2p^2} + 1 \right) \right\} \\ &= O\left(\frac{u^4}{X^2d^2} \sum_{p>u} \frac{1}{p^2} \right) + O\left(\sum_{p \leqslant 2u} 1 \right) \\ &= O\left(\frac{u^3}{X^2d^2 \log X} \right) + O\left(\frac{u}{\log X} \right) \end{aligned} \tag{31}$$

since $u > \frac{1}{2}\sqrt{X}$.

In (29) we use the estimates (30) or (31) according as the former or the second term in the latter is the lesser, or in other words by setting

$$\eta = \left(u^{\frac{3}{2}} \log^{\frac{1}{2}} X\right)/X,$$

which does not exceed $4u^2/X$. Hence

$$\begin{aligned} \sum\nolimits_u &= O\left(\frac{u^4}{X^2} \sum_{d>\eta} \frac{1}{d^2} \right) + O\left(\frac{u^3}{X^2 \log X} \sum_{d \leqslant \eta} \frac{1}{d^2} \right) + O\left(\frac{u}{\log X} \sum_{d \leqslant \eta} 1 \right) \\ &= O\left(\frac{u^4}{X^2\eta} \right) + O\left(\frac{u^3}{X^2 \log X} \right) + O\left(\frac{u\eta}{\log X} \right) \\ &= O\left(\frac{u^{\frac{5}{2}}}{X \log^{\frac{1}{2}} X} \right) + O\left(\frac{u^3}{X^2 \log X} \right) + O\left(\frac{u^{\frac{5}{2}}}{X \log^{\frac{1}{2}} X} \right) \\ &= O\left(\frac{u^{\frac{5}{2}}}{X \log^{\frac{1}{2}} X} \right) \end{aligned}$$

since $\xi_2 < X^2 \log X$ by (2), where it should be observed that the estimations are valid but trivial for the smaller values of u for which $\eta < 1$. Consequently

$$\frac{1}{u^2}\sum\nolimits_u = O\left(\frac{u^{\frac{1}{2}}}{X\log^{\frac{1}{2}} X}\right)$$

and we deduce from (2) again that

$$P_2'(X) = O\left(\frac{\xi_2^{\frac{1}{2}}}{X\log^{\frac{1}{2}} X}\right) = O\left(\frac{1}{\log^{\frac{1}{20}} X}\right),$$

which with (27) yields the estimate

$$P_2(X) = O\left(\frac{1}{\log^{\frac{1}{20}} X}\right).$$

Returning to (26) and (25), we extract the inequality

$$\mathcal{N}^{(4)}(X) < \frac{10AX^2}{C} \quad \big(X > X_0(C)\big) \tag{32}$$

we need.

7. The theorems

Inserting the inequalities (7), (8), (9), and (32) in the combinatorial inequality (4) for $N(X)$, we get

$$\frac{1}{X^2}\left|N(X) - 4X^2\prod_p\left(1 - \frac{\rho(p^s)}{p^{2s}}\right)\right| < \frac{13A}{C}$$

for $X > X_0(C)$, whence

$$\overline{\lim_{X\to\infty}}\frac{1}{X^2}\left|N(X) - 4X^2\prod_p\left(1 - \frac{\rho(p^s)}{p^{2s}}\right)\right| \leqslant \frac{13A}{C}$$

for any large constant C. Since the left-side above is independent of C, we therefore conclude that

$$N(X) \sim 4X^2\prod_p\left(1 - \frac{\rho(p^s)}{p^{2s}}\right)$$

as $X \to \infty$ and can thus state the following

Theorem 1. *Let us adopt the notations and hypotheses concerning the inhomogeneous polynomial $f(x, y)$ of degree r that were adopted in the Statement at the beginning of the paper. Then in case* (B)*, namely, in the case where $f(x, y)$ is a product of linear factors over some extension field of the rationals, we have*

$$N(X) \sim 4X^2\prod_p\left(1 - \frac{\rho(p^s)}{p^{2s}}\right) \tag{33}$$

as $X \to \infty$ provided that $s \geqslant \frac{1}{2}r - 1$.

As stated in the Introduction, the method of this paper can be used to extend Theorem 2 of I, which supplied an inequality in a situation that escaped the treatments of Greaves and Filaseta.

Theorem 2. *For the cube-free values of an irreducible binary octic form there is an asymptotic formula that is analogous to* (33) *in Theorem* 1.

References[2]

[1] C. Hooley, Applications of Sieve Methods to the Theory of Numbers, Cambridge University Press, 1976.
[2] C. Hooley, On the power-free values of polynomials in two variables, Roth 80th birthday volume, in press.

[2] For relevant citations of the work of other authors the reader is directed to the list of references in I.